

# 펌프-밸브 시스템의 DES 접근론적 Failure Recovery

손형일\*, 김기웅(부산대 대학원 지능기계공학과), 이석(부산대 기계공학부)

## DES Approach Failure Recovery of Pump-valve System

H. I. Son, K. W. Kim(Intelli. Mech. Eng. Dept., PNU), S. Lee(Mech. Eng. School, PNU)

### ABSTRACT

For the failure diagnosis of industrial system like various manufacturing systems, power plants and etc, many failure diagnosis approaches are considered. Here we are focus on the DES approach for failure diagnosis. We treats of failure recovery problem that is early not mentioned in DES approach. The procedure to design a recoverable diagnoser is presented. And the recoverability, necessary and sufficient condition for recoverability are defined. Then we make the high-level diagnoser to reduce the state size of recoverable diagnoser. Finally, a pump-valve system example is presented.

**Key Words** : Discrete Event Systems, Failure Diagnosis, Failure Recovery, Model Reduction

### 1. 서론

산업시스템의 고장진단은 지난 몇십년동안 많은 관심을 받아온 연구분야였다. 반도체 생산시스템, 자동차 생산시스템, 화학공정 시스템, HVAC (Heating, Ventilation and Air Conditioning) 시스템, 발전소등을 그 예로 들 수 있겠다.

근래에 들어 시스템이 대규모화되고 복잡해짐에 따라 고장진단을 위한 보다 조직적이고 체계적인 방법이 필요하게 되었다. 그래서 fault tree, analytical redundancy, expert system, model-based reasoning, Discrete Event System (DES)등을 이용한 많은 접근론들이 연구되고 있다. 이런 접근론들은 각각 다음과 같은 단점이 있다. 먼저 fault tree는 기본적으로 그것을 구성하기가 너무 어렵다. 그리고 analytical redundancy는 계산 복잡도가 크고, 모델링 오차와 계측 noise로 인해 sensitivity가 문제를 야기 시킨다. Expert system 역시 fault tree와 마찬가지로 구성하기가 너무 힘들다는 단점이 있다. 마지막으로 model-based reasoning은 많은 연구가 이루어지고 있지만 아직까지 dynamic 시스템에 대한 적용이 어렵다는 단점이 있다. 그렇지만 DES 접근법은 일반적으로 고장진단 할 대부분의 산업시스템이 DES로 생각될 수 있어 시스템을 모델링하기가 비교적 쉽고 고

장진단을 위한 보다 체계적인 방법을 제시하므로 고장진단을 위한 좋은 방법이 될 수 있다[1][2][3][4][5]. 이와 같은 이유로 [4][6]에서는 DES 접근법을 이용하여 고장진단 시스템을 구성하였다. 그리고 [5]는 [4]에서 제안한 diagnostic supervisor를 기초로 하여 [1][2][3]에서는 다루지 않은 failure recovery 문제를 다루었다. 이렇게 하여 diagnoser가 failure를 detect만 하는 것이 아니라 isolation과 recovery를 할 수 있게 만들어 diagnoser가 초기의 normal 상태로 되돌아가게 만들었고 이를 본문에서는 recoverable diagnoser라 명명하였다. 또 설계된 diagnoser의 state 개수를 줄여 high-level diagnoser를 설계하는 방법도 제시하였다.

본 논문에서는 [5]에서 제시한 방법을 간단한 펌프-밸브 시스템에 적용하였다.

### 2. Background

**정의 1** : Recoverable diagnoser가 초기화되고 임의의 failure mode  $F_i$ 가 발생한 후 임의의 event들이  $N_i$ 번 발생한 후 recoverable diagnoser의 state가  $F_i$ -certain이 되면 diagnoser는  $F_i$ -diagnosable하다고 한다. 그리고 모든 failure mode  $F_i$ 에 대해서  $F_i$ -diagnosable하다면 recoverable diagnoser는 *diagnosable*

하다.

◎

**정리 1** : Recoverable diagnoser에  $F_i$ -indeterminate cycle이 존재하지 않는다는 것은 diagnoser가  $F_i$ -diagnosable하기 위한 필요충분조건이다. ◎

**정의 2** : Recoverable diagnoser가 다음을 만족하면  $F_i$ -recoverable하다고 한다.

$$\forall (F_i - \text{certain}) z_R, RF_i \in \gamma_R(z_R) \quad \text{◎}$$

**정리 2** : 다음의 두 가지 조건은 recoverable diagnoser가  $F_i$ -recoverable하기 위한 필요충분조건이다.

조건 1) State condition이  $F_i$ 인 모든 recoverable DES의 state  $q_R$ 에서  $RF_i$ 가 enable될 수 있다.

조건 2) Recoverable diagnoser에  $F_i$ -indeterminate cycle이 존재하지 않는다. ◎

**정의 3** : Recoverable DES를 다음을 만족시키는 partition중 coarsest한  $\pi$ 에 의해서 재구성한 것을 **high-level DES**라 하자.

$$\pi \leq \ker \lambda \wedge \ker \gamma \wedge \ker x \quad \text{◎}$$

**정리 3** : Recoverable diagnoser  $D_R$ 과 high-level diagnoser  $D_{hi}$ 는 equivalent하다. ◎

### 3. Pump-valve System

#### 3.1 Recoverable DES Modeling

펌프, 밸브, supervisor로 구성되어 있는 간단한 펌프-밸브 시스템을 고려하자. 계측센서로는 flowmeter가 사용된다고 가정하자. Flowmeter의 값은 noflow를 나타내는 NF와 flow를 나타내는 F 두 개가 있다고 하자. 따라서 sensor output set  $Y_R = \{NF, F\}$ 이다. 펌프에는 고장이 발생하지 않고, 밸브에만 Stuck-closed의 고장이 발생한다고 가정하자. 여기서 failure event Stuck-closed를 failure mode  $F_1$ 으로 두자. 그리고  $F_1$ 에 대한 recovery event  $RF_1$ 을 두자. 그러면 펌프와 밸브에 대한 FSA 모델링은 그림 1과 같다. 펌프와 밸브의 초기 state는 각각 VC, POFF이다. 그리고 본 예제에서는 [6]에서와 다르게 밸브의 marked state set을  $\{VC, SC\}$ 가 아닌  $\{VC\}$ 로 잡았다. State SC에서 recovery event  $RF_1$ 이 일어나므로 blocking이 발생하지 않기 때문이다. 펌프의 marked state set은 물론  $\{POFF\}$ 가 된다.

시스템의 legal language는 그림 2와 같이 두고 DES의 FSMA를 구하면 그림 3과 같이 된다. 그림 3의 FSMA에 대한 control command map, sensor output

map은 표 1에 나타내었다.

#### 3.2 Recoverable Diagnoser

앞에서 정의한 펌프-밸브 시스템에 대한 state condition map은 표 1과 같다. 그리고  $q_8 = \delta(q_1, F_1)$ 이므로 recoverable diagnoser의 초기 state는  $\{q_1, q_8\}$ 이 되고 [5]에서 제시한 방법에 의해서 설계된 recoverable diagnoser는 그림 4에 나타내었다.

그림 4에서 state  $\{q_8, \{q_9, \{q_{10}, \{q_{11}\}$ 가  $F_1$ -certain이다. 그러므로 예제 1의 recoverable diagnoser는  $F_1$ -diagnosable하다. 그리고 물론  $F_1$ -indeterminate cycle도 존재하지 않는다. 즉, 그림 3을 보면 recoverable DES에서  $\{q_1, q_2, q_3, q_4\}$ 가 N-cycle을 이루고  $\{q_8, q_9, q_{10}, q_{11}\}$ 이  $F_1$ -cycle을 이루고 있지만, 그림 4의 recoverable diagnoser에서는  $F_1$ -uncertain state들이 cycle을 이루지 않으므로  $F_1$ -indeterminate cycle도 존재하지 않는 것이다. 따라서 정리 2에 의해서  $F_1$ -diagnosable하게 되는 것이다.

#### 3.3 Recoverability

그림 4의 recoverable diagnoser에서 state  $\{q_8, \{q_9, \{q_{10}, \{q_{11}\}$ 은 정의 8에 의해서  $F_1$ -recoverable하다. 왜냐하면 state  $\{q_8, \{q_9, \{q_{10}, \{q_{11}\}$ 은  $F_1$ -certain인 state이고  $\{q_8, \{q_9, \{q_{10}, \{q_{11}\}$ 에서  $RF_1$ 가 enable되기 때문이다. 그리고 그림 4에서  $F_1$ -certain인 state는  $\{q_8, \{q_9, \{q_{10}, \{q_{11}\}$ 밖에 없다. 또  $F_1$ -indeterminate cycle이 존재하지 않으므로 recoverable diagnoser는 정리 3에 의해서도  $F_1$ -recoverable하다고 할 수 있다. 즉 초기 state에서 control command Open\_valve, Start\_pump가 발생하고 sensor output이 NF가 나오면 state  $\{q_{10}\}$ 은  $F_1$ -certain이 되어 failure mode  $F_1$ 가 발생했는지 recoverable diagnoser는 알게되는 것이다. 그리고 state  $\{q_{10}\}$ 에서  $F_1$ -recoverable event  $RF_1$ 이 enable되므로 failure mode  $F_1$ 가  $RF_1$ 에 의해서 recover될 수 있게 되는 것이다.

### 4. High-level Diagnoser

#### 4.1 High-level DES

펌프-밸브 시스템에 대한  $\pi \leq \ker \lambda \wedge \ker \gamma \wedge \ker x$ 을 만족시키는 projection  $P_\pi$ 에 의해서 high-

level DES를 구하면 그림 5와 같다. 그림 5에서 보듯이 state  $(\{q_2\}, \{q_5\}), (\{q_3\}, \{q_6\}), (\{q_4\}, \{q_7\})$ 이  $\pi$ 에 대해서 coset이 된다. 즉 recoverable DES의 coset  $(\{q_2\}, \{q_5\}), (\{q_3\}, \{q_6\}), (\{q_4\}, \{q_7\})$ 이 high-level DES에서는 각각  $\{q_2\}, \{q_3\}, \{q_4\}$ 로 나타나는 것이다.

그리고 정의 9에서 알 수 있듯이 high-level DES는 state만을 partition하므로 recoverable DES state  $q_R$ 의 control command, sensor output은 변하지 않는다. 따라서 그림 5의 high-level DES에 대한 control command map  $\gamma_{hi}$ , sensor output map  $\lambda_{hi}$ 은 표 1에서 쉽게 알 수 있으므로 생략하겠다.

## 4.2 High-level Diagnoser

그림 5에 대한 high-level diagnoser를 만들면 그림 6과 같다. 그림 6의 high-level diagnoser는 그림 4의 recoverable diagnoser보다 state 수가 2개 줄어들었다. 그렇지만 high-level diagnoser도  $F_1$ -diagnosable,  $F_1$ -recoverable하므로 recoverable diagnoser와 같은 기능을 수행할 수 있다. 그리고 diagnoser에서 발생하는 control command 역시 같기 때문에 high-level diagnoser는 recoverable diagnoser와 equivalent하다.

## 5. 결론

본 논문에서는 DES 접근론적 failure diagnosis 문제를 다룸에 있어서 [4][6]에서 제시한 diagnostic supervisor에서 failure detection 문제뿐만 아니라 failure recovery 문제까지 다루었다. 우리가 제안한 recoverable diagnoser는 failure event를 detect한 후 시스템을 초기의 normal state로 되돌아가게 하여 보다 효과적인 failure diagnosis를 수행하게 된다. 그리고 supervisory control의 측면에서는 diagnostic supervisor에서 발생하던 blocking을 해결한 것이다. 하지만 failure recovery event를 DES에 추가시킴으로써 state의 수가 exponential하게 증가하게 된다. 이와 같은 이유로 recoverable diagnoser와 같은 state estimation을 수행하면서 보다 적은 수의 state 수를 가지는 high-level diagnoser의 설계방법도 제안하였다. 마지막으로 recoverable diagnoser와 그에 대한 high-level diagnoser가 equivalent함을 증명하여 high-level diagnoser의 유용성을 확인하였다.

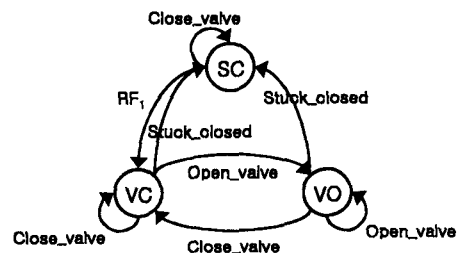
추후연구과제로는 nondiagnosable한 시스템을 diagnosable하게 변화시키는 active diagnosis 문제를 다루는 것을 들 수 있겠다. 그리고 시스템이 diagnosable하기 위한 최적의 센서 개수와 위치를 찾는 문제도 앞으로 다루어야 할 문제이다.

## 참고문헌

1. Meera Sampath, "A Discrete Event Systems Approach to Failure Diagnosis", Ph.D. Thesis, The University of Michigan, December, 1995.
2. M. Sampath, S. Lafortune, D. Teneketzis, "Active Diagnosis of Discrete-Event Systems", IEEE Trans. Automat. Contr., vol. 43, no. 7, pp. 908-929, July, 1998.
3. Shahin Hashtrudi Zad, "Fault Diagnosis in Discrete Event and Hybrid Systems", Ph.D. Thesis, The University of Toronto, 1999.
4. 손형일, 김기웅, 이석, "이산사건 시스템의 Failure Diagnosis", 제어계측, 로봇틱스 및 자동화 연구회 합동 학술 발표회 논문집, pp.298- 303, 2000.
5. 손형일, 김기웅, 이석, "이산사건 시스템의 Failure Recovery", 제어계측, 로봇틱스 및 자동화 연구회 합동 학술 발표회 논문집, pp.304- 309, 2000.
6. 손형일, 김기웅, 이석, "펌프-밸브 시스템의 DES 접근론적 Failure Diagnosis", 본지에 게재.

Table 1 Control Map  $\phi$ , Sensor Output Map  $\lambda$  and State Condition Map  $\chi$

State	Control Command $C$	Sensor Output $Y$	State Condition $\chi$
$q_1$	Open_valve	NF	$N$
$q_2$	Start_pump	NF	$N$
$q_3$	Stop_pump	F	$N$
$q_4$	Close_valve	NF	$N$
$q_5$	Start_pump	NF	$N$
$q_6$	Stop_pump	F	$N$
$q_7$	Close_valve	NF	$N$
$q_8$	Open_valve, $RF_1$	NF	$F_1$
$q_9$	Start_pump, $RF_1$	NF	$F_1$
$q_{10}$	Stop_pump, $RF_1$	NF	$F_1$
$q_{11}$	Close_valve, $RF_1$	NF	$F_1$



(a)

